GDPR

General
Data
Protection
Regulation

Overview

- What is the GDPR?
- What are the main changes?
- Risks?
- What do you need to do to be compliant?
- Data Breaches
- How does the GDPR affect you?
- Steps to Compliance
- Summary

HENDERSON LOGGIE
Chartered Accountants

What is the GDPR?

- The EU's General Data Protection Regulation (GDPR) aims to unify and strengthen the different data protection laws across member states. Will bring data protection legislation into line with new, previously unforeseen ways that data is now used.
- The current legislation was enacted before the internet and cloud technology created new ways of exploiting data, and the GDPR seeks to address that. By strengthening data protection legislation and introducing tougher enforcement measures, the EU hopes to improve trust in the emerging digital economy.
- The GDPR comes into force on 25 May 2018. Will result in significant changes in the current UK data protection law and a much tougher enforcement regime.
- Will still apply after Brexit – regulations incorporated into the Data Protection Bill (expected to be enacted later in 2018).
- The current limit for ICO fines is £500,000, however, this will increase to 20 million euros or 4% of revenue under GDPR.

What are the main changes?

Below are just a few of the key areas we need to consider where GDPR will strengthen or change the Data Protection Act:

- Requirement to appoint a **Data Protection Officer** (in certain cases – although is viewed as good practice in all others);
- Changes to how **consent** can be obtained from individuals for the use of their data. For example, data subjects will have to explicitly 'opt in' to allow their data to be shared, and it must be made clear to them exactly how their data will be used;
- The introduction of **new rights for data subjects**, including the right to be provided with a copy of their data so they can move it to another organisation (data portability) and the right to be forgotten (data erasure);
- GDPR is also clearer around the need to **ensure that data is being held only for the purpose that it was gathered**, and that it is also being deleted when it is no longer needed.

The Six GDPR Principles to Ensure Accountability

What do you need to do to be compliant?

- Once the legislation comes into effect, as a data controller, you must ensure **personal data is processed lawfully**, transparently, and for a specific purpose. Once that purpose is fulfilled and the data is no longer required, it should be deleted.
- 'Lawfully'? – Means the data subject has consented to their data being processed; or can mean to comply with a contract or legal obligation; or if doing so is in the controller's legitimate interest - such as preventing fraud.
- At least one of these justifications must apply in order to process data.

What do you need to do to be compliant?

- **Consent** must be an active, affirmative action by the data subject, rather than the passive acceptance under some current models that allow for pre-ticked boxes or opt-outs.
- Must keep a record of how and when an individual gave consent, and that individual may withdraw their consent whenever they want. If your current model for obtaining consent doesn't meet these new rules, you need to bring it up to scratch or stop collecting data under that model when the GDPR applies.

What do you need to do to be compliant?

- **Data breach response plan** - It's your responsibility to inform the ICO of any data breach that risks people's rights and freedoms within 72 hours of you becoming aware of it.
- Initial contact with ICO should outline the nature of the data that's affected, roughly how many people are impacted, what the consequences could mean for them, and what measures you have already actioned or plan to action in response.
- Before contacting the ICO need to tell the people affected by the data breach. Failure to meet the 72-hour deadline could result in a fine being imposed by the ICO, or a data processing restriction order being imposed.

Data Breach

- Fines just will not just apply to organisations. Depending on the circumstances relating to a data breach the ICO may seek to prosecute an individual if liability can be demonstrated.
- The existing Data Protection Act the ICO can prosecute under section 55 which provides *'a person must not knowingly or recklessly, without the consent of a data controller, obtain or disclose personal data (or the information contained in personal data) or procure the disclosure to another person of the information contained in personal data.'*
- Likely penalty is a fine plus costs.

Data Breach

- Definition of a personal data breach much broader, and includes:
  - ❑ access by an unauthorised third party;
  - ❑ deliberate or accidental action (or inaction) by a controller or processor;
  - ❑ sending personal data to an incorrect recipient;
  - ❑ computing devices containing personal data being lost or stolen;
  - ❑ alteration of personal data without permission; and
  - ❑ loss of availability of personal data.

How does the GDPR affect you?

- Even if you are a non-corporate body, such as club, society or even a small charity, you still have to comply with the GDPR. Your activities are likely to be limited to localised and specific fund-raising or hosting events. You may collect data for a mailing list, newsletter, or simply to inform members of what is happening.

- Relatively easy to comply with the GDPR and there is very little that you need to do – BUT, there is still some preparation required!

Steps to Compliance

Step 1:

- Make sure you have a process for collecting and storing data.
- Make sure you have someone whose job it is to follow that process. If you are a one-person or small organisation it does add a layer of work but you have to do this to be compliant.
- A flowchart of your processes will usually be enough and is then something you can pass on or show and others will be able to follow.
- Documenting your processing activity is mandatory.

Steps to Compliance

Step 1 (continued):

You must have a simple document, that you give to everyone, that explains:

- What data you collect (names and addresses etc.);
- Where and how it is stored;
- Who can view it and importantly what they can view;
- Any information that is shared with a third party - this includes data that you must supply to legal bodies;
- Give people a copy when they opt in, and make sure it is in simple and clear language.

Steps to Compliance

Step 2: Consent

- Have a consent form that asks people permission to store their details and what you do with those details. This is the 'opt in' or consent policy. You can make this consent policy part of your one page document but make sure that they have a copy and you have a signed copy.

Steps to Compliance

Step 3: Their rights

Make sure they have the right to:

- Be removed from the membership list;
- See what information you store (on them);
- Have history deleted (theirs);
- Change details.

The on-going concerns you will have is that you must let them know who has access to the membership list and why and any changes you make. This must be declared and their consent asked for, this includes when you make changes, you must ask for their consent again (before and not after).

Security

- You should also make sure any data is safely stored, if stored in an electronic format it should be on a computer that is patched, has the latest software/security software installed and if possible encrypted (most systems have this as an option).

- How you store their data, and the security of it, are your only real challenging legal issue. It does mean keeping a regular watch on your laptop/PC security to ensure they are up to date, but that is just good practice and common sense anyway in today's highly dangerous cyber environment.

Summary

- Most of your duties are easily solved with a one page document explaining your processes and how to contact people with a consent box and their signature (have two copies for each person, one for your records, one for them). You should detail your processes so that anyone can repeat them with a master guide to make sure the proper procedure is followed year on year.
- Having a single named person as the lead for data protection who can make sure this is all followed and kept up to date will help. There is, as previously stated, a little bit of work up front but once you have the process in place it should be easy to follow.